FEDERAL ELECTION COMMISSION
WASHINGTON, D.C. 20463

MEMORANDUM

November 29, 2018

TO: The Commission

THROUGH: Alec Palmer AP
Staff Director

FROM: Kimberly Humphries KH
Acting Deputy CIO - Operations

Justin Park JP
Acting Chief Information Security Officer

SUBJECT: Updated Corrective Action Plan for Disaster Recovery and COOP Audit

The attached Corrective Action Plan (CAP) has been updated to show the progress the Office of the Chief Information Officer has made since the last update. Significant progress was made during this time period, with the deployment of new surface tablets for COOP personnel and the completion of COOP training. We look forward to working with the OIG in the coming months to discuss recent progress in closing out the remaining items.

Please feel free to contact me if you have any questions.

Thank you.

Recommendation	Planned Corrective Actions	Status	Owner	Management Follow Up Notes November 2017	Revised Implementation Date
Project Name: T-Inspection of the FEC's Disaster Recovery and Continuity of Operations Plan					
Finding: Certification and Accreditation documents for the LAN risk assessment to support the system security plan (SSP) were not provided to the auditors for review.					
Conduct and document FEC's Certification and Accreditation package to include Security Controls Assessment (SCA)/Security Test and Evaluation (ST&E) in accordance with federal guidelines for information systems.	Concur with the recommendation 1 & 2. The FEC will solicit public bids for the accrediting and Certifying the FEC LAN , which will include the ST&E and SCA recommendations. Certification and accreditation for FEC major systems will be conducted during calendar year 2012 as funding becomes available. The LAN Risk Assessment was placed in PBC folder #2 on 1/10/13. Do not concur with recommendation 3, we will conduct C&A in accordance with the current policy. Do not concur with recommendation 4, testing and C&A are separate entities and the documentation will remain separate.	closed	Jay Ribeiro	Full ATO package for the GSS (FEC LAN) is tentatively scheduled to be completed July 2017. Full package will include updated SSP, SAR, POA&M, appointment orders and ATO recommendation memo. ST&E formal plan and A&A (formerly known as C&A) program was submitted to OIG on February 9, 2017.	ATO SIGNED AND COMPLETED *THIS CAP IS CLOSED*
Complete the development of the FEC Certification and Accreditation Program by March 2013, with certification of the FEC's major applications and general support systems being completed by April 2013. The C&A should be completed before placing systems into operation	Concur with the recommendation 1 & 2. The FEC will solicit public bids for the accrediting and Certifying the FEC LAN , which will include the ST&E and SCA recommendations. Certification and accreditation for FEC major systems will be conducted during calendar year 2012 as funding becomes available. The LAN Risk Assessment was placed in PBC folder #2 on 1/10/13. Do not concur with recommendation 3, we will conduct C&A in accordance with the current policy. Do not concur with recommendation 4, testing and C&A are separate entities and the documentation will remain separate.	closed	Jay Ribeiro	FEC Policy 58-2-4 was recently updated in accordance with NIST 800-37. A supplemental A&A workflow diagram has been formalized. As far as authorization of FEC's major applicaton and GSS - please see above. GSS and systems are in operation.The ATO package is tentatively scheduled to be completed July 2017. ST&E formal plan and A&A (formerly known as C&A) program was submitted to OIG on February 9, 2017.	FEC A&A program completed and submitted to OIG on Feb 9, 2017. Authorization of GSS and major applications (Web, Efiling and GSS are all completed *THIS CAP IS CLOSED*
Authorize (i.e., accredit) the information system for operations every two years (i.e. April 2013, April 2015, etc.).	Concur with the recommendation 1 & 2. The FEC will solicit public bids for the accrediting and Certifying the FEC LAN , which will include the ST&E and SCA recommendations. Certification and accreditation for FEC major systems will be conducted during calendar year 2012 as funding becomes available. The LAN Risk Assessment was placed in PBC folder #2 on 1/10/13. Do not concur with recommendation 3, we will conduct C&A in accordance with the current policy. Do not concur with recommendation 4, testing and C&A are separate entities and the documentation will remain separate.	closed	Jay Ribeiro	Assessment & Authorization (A&A) workflow has been formalized addressing the FEC ATO timeframe. According to NIST 800-37 rev. 1, "Authorization termination dates are influenced by organizational policies which 'may' establish maximum authorization period" (NIST SP 800-37, 2010). Supplemental In FEC's case, section 2.(g)., states "All FEC major applications and general support systems shall be re-authorized when modified or upgraded in a way that impacts information security and assurance, or in response to changes in the risk environment. In the absence of modifications or upgrades, re-authorizations will be performed when deemed necessary by the FEC CIO (FEC Policy 58-2.4, 2017). The FEC LAN is currently undergoing re-authorization process. FEC Assessment and A	COMPLETED

	Develop a security test and evaluation plan, implement the plan, and document the results as part of the C&A package.	Concur with the recommendation 1 & 2. The FEC will solicit public bids for the accrediting and Certifying the FEC LAN , which will include the ST&E and SCA recommendations. Certification and accreditation for FEC major systems will be conducted during calendar year 2012 as funding becomes available. The LAN Risk Assessment was placed in PBC folder #2 on 1/10/13. Do not concur with recommendation 3, we will conduct C&A in accordance with the current policy. Do not concur with recommendation 4, testing and C&A are separate entities and the documentation will remain separate.	closed	Jay Ribeiro	The test plan has been formally signed on January 24, 2017 to start assessment work on 2/13/17. The FEC General Support System (GSS) is currently undergoing ST&E as part of the C&A package. The ST&E is tentatively scheduled to be completed on 4/12/17 and a POA&M will be generated as a result of the assessment. The Security Assessment Report (SAR), updated System Security Plan (SSP) and the Plan of Action & Milestone (POA&M) will all be generated as part of the Authorization Package.	COMPLETED
Finding: An alternate workspace has not been secured in the event of a disaster.						
	Develop and implement a Memorandum of Understanding (MOU) with GSA to secure an alternate workspace in accordance with the COOP in case of a disaster at the FEC building by February 2013.	The FEC has attempted to establish this MOU, in FY2009. The CFO contacted GSA to established this arrangement but was rebuffed by GSA. GSA stated that in the event of a national emergency alternative office space availability is determined by national disaster recovery prioritization. GSA further stated that in the event of a FEC specific and unique disaster, office space will be provided at the time, this is part of GSA's mission and will be conducted at the time of disaster rather than in advance. No further action required	closed	Kim Humphries	Management maintains its current position.	Per discussion, this can be closed out.
Finding: COOP and DRP training is not provided to key COOP personnel.						
	We recommend FEC ITD develop and implement a Training Program. Training for key personnel with contingency plan responsibilities should focus on familiarizing them with COOP roles and teaching skills necessary to accomplish those roles. Key personnel should be trained on the following plan elements: • Cross-team coordination and communication; • Reporting procedures; • Security requirements; • Team-specific processes (Activation and Notification, Recovery, and Reconstitution Phases); and • Individual responsibilities (Activation and Notification, Recovery, and Reconstitution Phases).	Concur with the recommendation 1 in part. The FEC should and will develop a COOP/DR training plan that is commensurate with the level of COOP/DR as necessary for the DR category and resources available to this agency. Do not concur with recommendation 2 in that training should be conducted annually. Our training plan will provide training as personnel change.	closed	Kim Humphries	Management agrees to enact a yearly training/certification program for COOP personnel to identify expectations and procedures on a high level. Team specific functions and processes to continue operations in a COOP scenario will reflect the same functions and processes performed as part of the team's weekly telework procedures.	Training completed May 2018
	We recommend that COOP/DRP training is provided at least annually. Personnel newly appointed to COOP roles should receive training shortly thereafter joining the FEC if training has already been conducted for the year.	Concur with the recommendation 1 in part. The FEC should and will develop a COOP/DR training plan that is commensurate with the level of COOP/DR as necessary for the DR category and resources available to this agency. Do not concur with recommendation 2 in that training should be conducted annually. Our training plan will provide training as personnel change.	closed	Kim Humphries	Management agrees to enact a yearly training/certification program for COOP personnel to identify expectations and procedures on a high level. Team specific functions and processes to continue operations in a COOP scenario will reflect the same functions and processes performed as part of the team's weekly telework procedures.	Training will occur once a year in May
Finding: FEC does not have Interconnection Security Agreements (ISA) for external systems.						
	Authorize connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements with Savvis.	The FEC has a service level agreement in place. This document was placed in PBC folder #15 on 1/11/13 for the audit review. The agreement with NFC is held on file with the CFO office I will provide the agreement by 1/30/2013. The FEC will pursue an agreement with the Senate if appropriate. The connection between the FEC and Senate is not a T1 line as stated in this NFR, but is a secure VPN tunnel connection direct to the Senate.	closed	Jay Ribeiro	This has been successfully addressed by management and the auditors have no additional comments. ISAs for Savvis was provided to OIG Feb 9, 2017.	Completed

	Document, for each connection, the interface characteristics, security requirements, and the nature of the information communicated	The FEC has a service level agreement in place. This document was placed in PBC folder #15 on 1/11/13 for the audit review. The agreement with NFC is held on file with the CFO office I will provide the agreement by 1/30/2013. The FEC will pursue an agreement with the Senate if appropriate. The connection between the FEC and Senate is not a T1 line as stated in this NFR, but is a secure VPN tunnel connection direct to the Senate.	closed	Jay Ribeiro	This has been successfully addressed by management and the auditors have no additional comments. ISAs for Savvis, NFC and Salient was provided to OIG Feb 9, 2017.	Completed
	Monitor the information system connections on an ongoing basis verifying enforcement of security requirements	The FEC has a service level agreement in place. This document was placed in PBC folder #15 on 1/11/13 for the audit review. The agreement with NFC is held on file with the CFO office I will provide the agreement by 1/30/2013. The FEC will pursue an agreement with the Senate if appropriate. The connection between the FEC and Senate is not a T1 line as stated in this NFR, but is a secure VPN tunnel connection direct to the Senate.	closed	Jay Ribeiro	This has been successfully addressed by management and the auditors have no additional comments. ISAs for Savvis, NFC and Salient was provided to OIG Feb 9, 2017.	Completed
Finding: FEC has not resolved significant deficiencies identified in the COOP Alert section.						
	Within the fiscal year 2013, ending September 30, 2013, develop and implement test plans to fully test each program offices' COOP, with a target of completing all offices' testing by December 2013.	Concur with all recommendations. The FEC will develop a test plan to fully test the COOP/DR - March 2013. The FEC will test the COOP by the end of 2013. The FEC will develop a COOP training plan.	closed	Kim Humphries	Test plans for each program office is no longer necessary as each office will continue operations during the inactment of a COOP in the same manner in which they operate as part of the team's telework procedures.	
	Within the fiscal year (FY13), develop and implement a test plan to fully test the ITD DRP, with a target date to begin testing on or before June 2013.	Concur with all recommendations. The FEC will develop a test plan to fully test the COOP/DR - March 2013. The FEC will test the COOP by the end of 2013. The FEC will develop a COOP training plan.	open	Kim Humphries	Management agrees to devise a test plan and test the ITD DRP however, at this time, management believes it would be premature to devise this test plan until the newly acquired replication system is completely configured and online to determine what functions/processes need testing and how often.	Utilizing the features of our replication system, we have conducted market research and found a product that allows us to test our DRP in an orderly and systematic fashion. This would be a phased approach expecting full implementation to occur first quarter 2020.
	FEC should ensure that the COOPs are tested on an annual basis	Concur with all recommendations. The FEC will develop a test plan to fully test the COOP/DR - March 2013. The FEC will test the COOP by the end of 2013. The FEC will develop a COOP training plan.	closed	Kim Humphries	Management does not agree and believes testing of the COOP on an annual basis is no longer necessary as operations will follow the same procedures as part of the team's telework procedures.	
	Procure the necessary hardware/software to fully test the data entry application needed for Disclosure by December 2013	Concur with all recommendations. The FEC will develop a test plan to fully test the COOP/DR - March 2013. The FEC will test the COOP by the end of 2013. The FEC will develop a COOP training plan.	open	Kim Humphries	Management agrees to devise a DR test plan for Disclosure and fully test said plan however, at this time, management believes it would be premature to devise this test plan until the newly acquired replication system is completely configured, and online to determine what functions/processes need testing and how often.	We conducted a review of this system and determined we do not need to purchase systems. Test plans will be updated for this system in conjunction with updating the test plans for DR. Revised Implementation Date - 1st quarter 2020

	Ensure the disaster recovery Kofax server is updated to mirror the Kofax production server by June 2013.	Concur with all recommendations. The FEC will develop a test plan to fully test the COOP/DR - March 2013. The FEC will test the COOP by the end of 2013. The FEC will develop a COOP training plan.	open	Kim Humphries	Management agrees to devise a DR test plan for Kofax and fully test said plan however, at this time, management believes it would be premature to devise this test plan until the newly acquired replication system is completely configured, and online to determine what functions/processes need testing and how often.	We've devised a plan in theory which we are working to validate which may/may not require a server. Test plans will be updated for this system in conjunction with updating the test plans for DR. Revised Implementation Date - 1st Quarter 2020
Finding: FEC ITD Disaster Recovery Site does not have backup media readers to restore the backup tapes						
	We recommend that FEC install and test a backup media reader in the alternative disaster recovery site.	Concur with recommendation. The FEC will install and test a backup media reader at the DR site. As resources become available.	open	Kim Humphries	Management will obtain refreshed quotes and assess if equipment is necessary due to design changes in the OCIO Infrastructure.	With the implementation of our replication system and after performing market research we've determined a backup media system is not the most efficient way to conduct backups during a DR. We are looking at cloud-based solutions that would only incur costs if/when DRP is enacted.
Finding: FEC ITD has not developed and implemented a COOP exercise plan.						
	Develop and implement a COOP exercise plan. The functional exercise should include all COOPs points of contact and be facilitated by the system owner or responsible authority. Exercise procedures should be developed to include an element of system recovery from backup media	Do not concur with recommendation. The FEC has exercised the COOP/DR program, through "real exercise." The FEC has experienced server outages, power interruptions, and natural disasters that interrupt services from time to time. During these outages, we have switched from the production environment to the DR environment and proved that service will continue in the DR environment during the outages. The benefit of a scheduled test in addition to the fore mentioned outages, does not outweigh the cost of conducting an exercise, i.e.: downtime, overtime, lack of staff availability, and increase contract support costs.	Closed		Test plans for each program office is no longer necessary as each office will continue operations during the inactment of a COOP in the same manner in which they operate as part of the team's telework procedures.	Per discussion, this can be closed out.
Finding: FEC's COOP and DRP contact lists are outdated and do not contain adequate contact information.						
	Update all Continuity of Operation Plan (COOP) and Disaster Recovery Plan (DRP) personnel contact information to reflect the most current information and distribute the updated plans to the appropriate officials by February 2013.	Concur with all the recommendations. The Fec will update contact lists and COOP/DR policy to incorporate the recommendation.	closed	Kim Humphries	Management has updated the COOP list as part of its phased approach.	COMPLETE
	Implement and document a policy that includes: • Who is responsible for updating and monitoring the contact information in the FEC's COOPs and DRP to reflect current information; • An organization-defined frequency for updating the FEC's COOP/DRP contact information; and • "Required" information that must be provided for those personnel with COOP responsibilities (i.e. FEC office#, FEC blackberry#, personal cell phone and/or home number).	Concur with all the recommendations. The Fec will update contact lists and COOP/DR policy to incorporate the recommendation.	open	Kim Humphries	Management needs time to review the current process for updating the COOP/DRP afterwhich it will inact changes in processing, if necessary, and move forward with updating information in both plans.	Seeking outside assistance with updating COOP. Revised implementation date is third quarter 2019

For those FEC personnel who are unaware of their COOP responsibilities due to the FEC's failure to update their COOP/DRP contact information (i.e. Procurement Director), provide a copy of the plan with their associated responsibilities by February 2013.	Concur with all the recommendations. The Fec will update contact lists and COOP/DR policy to incorporate the recommendation.	closed	Kim Humphries	A copy of the plan will be distributed to COOP personnel once it has been updated.	A copy of the plan was made available to COOP Team members as part of COOP Training.
Finding: FEC's disaster recovery site and primary data site are in the same geographic area					
Review and obtain another alternative for the disaster recovery site or primary data site to ensure that the new facility is located in a geographic area that is unlikely to be negatively affected by the same disaster event (e.g., weather-related impacts or power grid failure).	The FEC accepts the risk that is associated with having the production and DR site in the same geographical location, but in separate facilities. Additionally there is a geographically separated mission essential production site to further protect productions data. FEC management deems this acceptable for the mission, disaster category, and resources of the agency. No further action required.	closed	Kim Humphries	Management maintains its current position and accepts this risk.	
Finding: Key personnel have not received a hard copy of the COOP and/or the file on a USB storage device to use during a disaster.					
Comply with FEC IT policy and provide hardcopies, along with USBs, of the COOPs to recovery personnel for use when they cannot access the servers where the COOP files are stored	Do not concur with recommendation. The COOP/DR plans are available to all personnel on a shared drive. It is the individual responsibility of each COOP/DR team member to obtain a copy of the plans as they see fit to fulfill their duties as team members. The FEC will, however emphasize this individual responsibility and incorporate in the training program agreed to in NFR 4 above.	closed	Kim Humphries	Management maintains its current position as COOP staff have been equipped with a tablet to ensure they have a device readily available to access the servers.	
Maintain a record of the individuals who received hard copies of the COOP and/or copies of the COOP files on USB devices	Do not concur with recommendation. The COOP/DR plans are available to all personnel on a shared drive. It is the individual responsibility of each COOP/DR team member to obtain a copy of the plans as they see fit to fulfill their duties as team members. The FEC will, however emphasize this individual responsibility and incorporate in the training program agreed to in NFR 4 above.	closed	Kim Humphries	Management maintains its current position.	
Contracts with vendors (SLAs and other contracts), software licenses, system user manuals, security manuals, and operating procedures should be stored with the plan.	Do not concur with recommendation. The COOP/DR plans are available to all personnel on a shared drive. It is the individual responsibility of each COOP/DR team member to obtain a copy of the plans as they see fit to fulfill their duties as team members. The FEC will, however emphasize this individual responsibility and incorporate in the training program agreed to in NFR 4 above.	open	Kim Humphries	Contracts with vendors are stored centrally on the Enterprise Content Management server and accessible by various COOP team members. Due to the constant updates and changes to vendor manuals and operating procedures, management believes it would be best to reference the vendor's website within the COOP/DR Plan to receive the most up-to-date information.	The DRP will be updated with vendor URL after the COOP has been updated. Tentative implementation date for updated DRP scheduled for fourth quarter 2020.
Finding: Security Control Assessment including the Security Test and Evaluation, and Plans of Action and Milestones has not been documented.					
We recommend that FEC conduct and document its Security Controls Assessment (SCA)/Security Test and Evaluation (ST&E) in accordance with federal guidelines for information systems	Concur with both recommendations. The FEC will solicit public bids for the accrediting and Certifying the FEC LAN , which will include the ST&E and SCA recommendations. Certification and accreditation for FEC major systems will be conducted during calendar year 2012 as funding becomes available.	closed	Jay Ribeiro	This has been successfully addressed by management and the auditors have no additional comments. ST&E approved plan was submitted to OIG on 9 Feb 2017.	COMPLETE

	Once the ST&E is complete, develop a POA&M to document the corrective action plan for remediating any findings	Concur with both recommendations. The FEC will solicit public bids for the accrediting and Certifying the FEC LAN , which will include the ST&E and SCA recommendations. Certification and accreditation for FEC major systems will be conducted during calendar year 2012 as funding becomes available.	closed	Jay Ribeiro	The FEC LAN is currently undergoing an independent Security Controls Assessment/Security Test and Evaluation (ST&E). The rules of engagement for the Security Assessment has been formally signed on January 24, 2017 to start assessment work on 2/13/17. The ST&E is tentatively scheduled to be completed on 4/12/17 and a POA&M will be generated as a result of the assessment. The Security Assessment Report (SAR), updated System Security Plan (SSP) and the Plan of Action & Milestone (POA&M) will all be generated as part of the Authorization Package.	COMPLETE
Finding: System Security Plan, COOPs, and DRP are not reviewed and updated on an annual basis						
	Review and update the FEC System Security Plan at least annually.	Concur in principle with the recommendation 1. The FEC will review and update the SSP, COOP and DRP annually, and document that such a review was held. Do not concur with recommendation 2, since we do not concur with annual training.	closed	Jay Ribeiro	This has been successfully addressed by management and the auditors have no additional comments.	COMPLETE
	Establish a process to certify that the COOPs for the FEC program offices and ITD's Disaster Recovery Plan (DRP) are updated on an annual basis to reflect changes in the information system environment and security controls in conjunction with the required annual training.	The General Support System (GSS) System Security Plan will be reviewed and updated annually as part of the NIST Risk Management Process. The COOP coordinator will be notified if and when updates to the information systems environment and security controls affects the COOP and DRP. According to the FEC Mandatory COOP Training, FEC will engage in yearly tabletop exercises. COOP members are required to complete an annual COOP training and certification through skillport.	open	Justin Park	Currently reviewing COOP plan	GSS System Security Plan (SSP) has reviewed. COOP Training completed May 2018 and will occur once a year in May. Currently reviewing COOP plan. Revised implementation date is third quarter 2019
Finding: The COOP pre-positioned equipment inventory should not be stored at the FEC office.						
	Store the pre-positioned equipment inventory in a geographic area that is unlikely to be negatively affected by the same disaster event (e.g., weather-related impacts or power grid failure) as the FEC office.	Concur with recommendation with reservation. Implementing this recommendation is predicated on the availability of funds	closed	Kim Humphries	Management provides each member of the COOP Team with a tablet, so there is no need to store pre-positioned equipment.	New tablets will be distributed to staff by 1st quarter 2018